"APPARATUS FOR CONTROL AND CERTIFICATION OF THE DELIVERY OF GOODS OBJECT OF ELECTRONIC COMMERCE AND FOR THE CONCURRENT CONTROL AND CERTIFICATION OF THE EXECUTION OF THE RELATED PAYMENT."

DESCRIPTION

The present invention provides an apparatus for control and certification of the delivery of goods object of electronic commerce and for the concurrent control and certification of the execution of the related payment.

For "electronic commerce" it is to be understood not only the purchasing of goods delivered "electronically" (e.g., a document) but also the electronic ordering of goods delivered through distribution channels of a non-computerized type.

For POS (Point of Sale) a system allowing purchase by means of "electronic money" using a card having a magnetized strip, a microprocessor or both or even the mere identification number, usually of 16 digits, of a card (cash card, credit card or others) is understood. Such card will be indicated herebelow with the generic term of electronic card, for ease of reference.

The POS system includes a plurality of elements, some (A1 to A10) placed on the user side, others (B1 to B5) on the side of the company issuing the electronic card:

A) USER SIDE

1) An electronic card reading device;

2) a data inputting device (keypad);

3) a displaying device;

4) a printing device;

5) a modem;

6) a software for the processing of the data read by the reading device (bank or credit company code, client code etc.). Data are stored in a buffer for subsequent comparisons. The company code is used to determine the identification number of a company issuing electronic cards to which one can connect. The client code will instead be used to operate the related monitoring, once the connection to the company issuing the electronic cards is obtained;

7) A data processing software for the data input. The amount entered through the keypad (or directly acquired from a cash register) is also stored in a buffer to be sent later to the company issuing electronic cards for the debiting procedure;

8) A software for the processing of the data entered by the user (personal secret code), including an encrypting module. Following the entering of a code on the keypad, a module specially provided for the purpose masks the entered digits, replacing them on the display with asterisks, while a further module applies an encrypting algorithm to the entered code. Then the code thus encrypted is stored in a buffer to be sent later on to the company issuing electronic cards for the monitoring procedure;

9) A data transmission software. Usually a communication software of commercial type (based on standard protocols of the TCP/IP type or the like) is used, sending the above mentioned stored data to the center modem by means of the modem mentioned at 5); and

10) A software for data receiving and interpretation. In this case as well, for the receiving usually a communication software of a type on the market (based on standard protocols of the TCP/IP type or the like) is used. The interpretation provides instead a software that, depending on the sequence of the received data, stores the various elements (amount, client code and secret code) in buffers. A decrypting module is also provided.

B) ELECTRONIC CARD ISSUING COMPANY SIDE

1) A telephone calls receiver, typically a device capable of modulating several telephone lines, e.g., an ISDN trunk;

2) A dedicated processor, with the related peripheral devices;

3) A database containing information over the cardholders, codes, granted credit, thefts/losses and the like;

4) A software for interrogation and authorization to conclude the transaction. In particular, by means of the client code, the database is first of all interrogated to access fields reporting stops, thefts etc. Then the database is interrogated to access fields containing the ceiling reserved to the user holder of the card and the amounts already spent. If everything is in order (the card is not stolen, expenditure amount not exceeding the daily withdrawing limit, sum of the amounts already spent and of the new amount within the monthly withdrawing limit) then the amount of the expense that is being operated at that time is summed to the monthly and daily expenses fields. Then the transaction is concluded successfully, with the generation of an "OK" code to be forwarded to the remote POS terminal; and

5) A software for forwarding along the telephone line of the caller the answer computed at the preceding point. Usually, a communication software of the commercial type is used here as well (based on standard protocols of the TCP/IP type

or the like) forwarding the "OK" code to the remote POS terminal that had activated the request through the modem.

The operation modes of the entire system of the known art hereto listed element by element will be disclosed herebelow with reference to the flow chart of figure 1:

In a first step D1 the operator inserts the card in the reading device.

In a second step D2 the data processing software mentioned at the previous A6 acquires the information stored in the card (bank or credit company code, client code etc.).

In a successive decision step D3 the card is recognized or not recognized.

If it is recognized, the flow proceeds to the steps D4 and D5 wherein respectively the manual or automatic entering of the amount to be paid and of the secret code are requested.

In a successive decision step D6 the secret code is recognized or not recognized, always by means of the software mentioned at the previous A6.

In a successive step D7 the acquired information is forwarded to the card issuing company center. Said information includes the client code, the amount to be paid, the identification number of the caller and whatever else is needed to be processed at the card issuing company side.

In the subsequent steps the card issuing company center acquires the request, processes it and sends the answer to the caller.

In particular, in step D8 is verified whether the data of the provider authorize the transaction or not. If it is authorized, in a step D9 the debiting of the cost on the provider side occurs. In a successive step D10 the acquiring of the affirmative answer by the caller occurs, while in a successive step D11 the printing of the slip confirming the transaction conclusion occurs. If instead the transaction is impossible (step D12) the printing or the displaying of the reason because of which the transaction could not be concluded can occur.

The transaction successfully concluded ends instead with the delivery of the goods by the operator (step D13).

A system as the one hereto described, at the moment adopted by nearly all stores and sales centers, cannot easily apply to the field of electronic trade, i.e., to the field related to the remote electronic purchasing of items or goods by means of network connection and on-line payment by electronic card. In fact, one of the main reasons making such a system impractical is its intrinsic need of providing

the presence of an operator, somehow certifying the successful conclusion of the transaction.

The electronic trade systems known to date provide the simple entering of the credit card identification number and the forwarding thereof through the Internet, Intranet, Extranet nodes or the like. The problems entailed to said mode are well known: on one hand the unwillingness of the user to let his credit card number travel along a system as the Internet, still not very safe, on the other hand, the service provider problem of making in real time an assessment of the validity or not of the credit card number that is being forwarded. Furthermore, the knowledge of the card number by the provider can bring to the automatic debiting of a monthly fee after a trial period or other uses by the provider that could hardly be controlled by the client, who can realized it only when checking the statement of account. Another known mode is that of providing the payment by means of cards of the prepaid type (e.g., telephone cards, rechargeable cards, prepaid highway-toll cards etc.). The problems related to the use of said cards concern first of all the value thereof, necessarily limited (in fact, being of the payable to bearer kind they are like cash, hence entailing the same risks of loss or theft of a bank note). Furthermore, said cards being of the scaling down kind, the user will never be certain of disposing of a residual amount sufficing for the purchase to be operated. Moreover, said cards need to be recharged (or repurchased) and therefore POS specially provided for the purpose have to be envisaged, the widespread distribution on the territory and availability (working hours) thereof being critical factors. Furthermore, the prepaid cards are issued by specific service providers (In Italy: Telecom, TIM, Società Autostrade etc.), thus allowing access to the services provided by the issuer only, in absence of specific agreements with other service providers.

However, the present invention will be able to use the present prepaid card payment systems, thus providing customers with a further possible alternative to execute the payment.

The present invention overcomes the drawbacks of the known art as it makes the POS system hereto described applicable to the systems of electronic commerce, further allowing the concurrent documentation of the operated transactions, with no need of providing an operator.

Moreover, by means of the present invention, data related to the credit card are not made to transit along Internet nodes, but forwarded through different telephone lines, such as for example those already in use with the POS system,

ensuring in this respect a data safety at least equaling that of the present POS systems.

By means of the present invention it will no longer be necessary to send identifications (numerical codes) relative to a payment system on the Internet, but it will be possible to fully separate the applicative transaction step in Internet (or Intranet, Extranet or other communication data networks) from the "negotiation" step of the payment: such step is run using direct communication channels (telephone lines and ISDN, TAC, GSM and satellite lines, radiofrequence etc.).

The present invention allows the certification of the conclusion of the payment process which took place through those lines and the communication thereof via Internet to the provider who will provide his service, being certain of having been paid.

In the following description reference will be made to the D ISDN channel as direct communication channel for the payment step: such choice is a mere example, as it is possible to use any of the available direct communication channels (mobile or household telephones, radio etc.)

A peculiar case that might occur when this invention is used without having another communication channel available, concerns the use of the same communication channel used for the access to the Internet: in this case by means of the present invention it will be possible to store the necessary data, disconnect from the Internet, use the communication channel to perform the payment, store the payment data, connect again to the Internet, re-establish the connection with the provider and complete the transaction by furnishing the data relative to payment. Furthermore, as an alternative to the disconnection to the communication channel, it will be possible to use, for the payment step, the same communication channel used for the Internet connection, made "safe" for the communication using methods known in the art (i.e. "tunneling").

In fact, the present invention provides an apparatus for control and certification of the delivery of goods object of electronic commerce by means of Internet, Intranet, Extranet connections or the like and for the concurrent control and certification of the execution of the related payment, comprising:

a) a system for reading an electronic card and for managing authorization processes by the electronic card issuing company(26, 28, 30, 31);

b) an apparatus (27) for monitoring and interpretation of application protocols for network data transmission systems connected to said system for reading an electronic card and comprising:

b1) a data packets monitoring device (9) at a layer corresponding to the OSI layer 2, said data packets comprising control frames and information frames, wherein the control and information frames contain a header portion and a body portion, said header portion for the distinction between an information frame and a control frame;

b2) a control unit (15) receiving as an input the data coming from the monitoring device (9) and comprising means for the discrimination of the control frames from the information frames;

b3) a dating unit (16) connected to the control unit (15) and associating a monitoring time to the control frames and to the information frames;

b4) a discriminated data storing unit (17) storing the control and the information frames and the monitoring time thereof, bidirectionally connected to the control unit (15);

b5) a predetermined data storing unit (18), bidirectionally connected to the control unit (15), said predetermined data representing possible interpretations of the information frames contained in the discriminated data storing unit (17);

b6) means for comparing, by the control unit (15), said predetermined data stored in the storing unit (18) with the data contained in the body portion of the information frames stored in the discriminated data storing unit (17), thus reconstructing the information frames according to their specific application syntax;

b7) means for ordering, according to the time and kind of communication, the information frames reconstructed according to their specific application syntax, thus reconstructing application sequences occurred between a determined source processor and a determined destination processor; and

b8) means for ordering said information frames ordered according to the time and kind of communication also according to a logical criterion, thus reconstructing the logical path of said application sequences occurred between a determined source processor and a determined destination processor, and

c) a data storing unit of the various transactions object of electronic commerce monitored and interpreted by means of said apparatus (27) for monitoring and interpretation of application protocols.

The control and the analysis of the data contained in the data storing unit allow to reconstruct the actual operation mode of the transactions so as to settle possible disputes. When needed, data stored in said storage unit might be encrypted by means of encrypting algorithms. The unit might further be lead-sealed.

Advantageous embodiments of the present invention will be provided in the dependent claims thereof.

The procedure is of automated type; in fact, the attendance of an operator is not needed, as the client wishing to operate the purchasing will be capable to complete the entire purchasing process with the sole aid of the apparatus according to the present invention.

The apparatus according to the present invention ensures that the goods are not delivered if the payment is not confirmed, as well as that the goods correspond to the order, and lastly that the amount paid corresponds to the one asked for.

Moreover, the apparatus according to the present invention can document in detail all the operated transactions. Thus, certified information is made available, capable of settling possible disputes.

Various operation modes of the present invention are listed herebelow:

1) Electronic commerce without a teller: the need of a conventional POS operator is eliminated, since the control of the payment and of the delivery of goods is made possible.

2) Authentication of remote bank transactions: in fact, a known type of electronic commerce provides an electronic interaction between an account holder and his own bank. By means of the present invention, once the client is identified by means of his electronic card, the operated transactions will be confirmed and documented.

The identification of the client holder of a electronic card can be further controlled through the remote recognition of the fingerprint or the acquisition of the image of the client by camera.

3) Recognition and authentication of operators provided with electronic card, who connect to a service center authenticating their identity, authorizing them to operate.

4) Electronic commerce via Intranet, Extranet and Internet. It allows to obtain the following advantages:

a) for the purchaser:

a1) entrusting the card number for payment to a transmission line different from the one used for the connection to Internet: card-related data will transit through the central switching systems (fixed lines, mobile lines or satellite lines), but not through the Internet web nodes, or the provider nodes. In this way, the card number is not sent to the service provider, thus avoiding possible undesired debiting;

a2) using the established safety standards of the methods and machinery used by the POS;

a3) obtaining a certification and a documentation of the operated transactions that can be used to settle disputes;

a4) a further control of the trade operated from each single location, in case of local networks connected to geographical networks through a single network processor;

b) for the service provider:

b1) to be certain of payment: the transaction is forwarded only after availability is controlled by the card issuing companies. Thus, the problems related to cards which have been stolen, revoked and so on are solved;

b2) obtaining certification and documentation of the operated transactions, to be used to settle disputes.

The present invention will be illustrated herebelow by referring to a preferred embodiment thereof, explained by way of a non-limiting example. Reference will be made to the figures of the annexed drawings, wherein:

figure 1, as set forth above, is a flow chart related to the operation of a POS of the known art;

figure 2 shows a schematic view of the OSI standard;

figure 3 shows a schematic view of the kind of data used on communication network;

figure 4 shows a block diagram of a component of the apparatus according to the present invention;

figure 5 shows a flow chart explaining the operation of the component in figure 4;

figures 6 and 7 show additional flow charts for the understanding of what described with reference to figure 5;

figures 8A and 8B show an example of an application tree containing statistical information obtained by means of the component in figure 4;

figure 9 is a block diagram of the apparatus according to the present invention; and

figures 10A and 10B are flow charts related to the operation of the apparatus according to the present invention.

Data transmission from a source device to a destination device can occur in different manners. However, to ensure a data exchange having the lowest possible chance of errors it is necessary to adopt a series of rules or control procedures. Said rules or procedures are known as "communication protocols".

A well known communication protocol is the "Open System Interconnection" (OSI) of the International Standards Organization (ISO). Said protocol is divided into seven layers, shown in figure 2. Layer 7 (application) on the source side contains information related to the sole message (M) to be sent to the destination side. The successive layers on the source side add control information to the message: layer 6 (presentation) divides the data of the original message into blocks (M1 and M2); layer 5 (session) adds a title (S) to indicate the sender, the receiver and some information related to the sequence; layer 4 (transport) adds information (T) related to the logic connection between the sender and the receiver; layer 3 (network) adds information related to the path (N) and divides the message into packets representing the standard communication unit in a network; layer 2 (data link) adds a title portion (B) and a tail portion (E) to the message to ensure the correct order of the various packets and to correct transmission errors; the single message bits and control information bits added by the various layers are transmitted on the physical medium through layer 1. The downward pointing arrow F1 on the sender side indicates the manner according to which the outgoing message is constructed. Every addition to the message is verified and removed from the corresponding layer on the destination side. The upward pointing arrow F2 on the destination side indicates the manner according to which the incoming message is reconstructed.

The OSI model schematically described up to this point is just a conceptual model. A typical protocol normally adopted in the transactions related to the electronic trade is the protocol TCP/IP (Transmission Control Protocol and Internet Protocol). Said protocol, just like other communication protocols adopted, can be explained with reference to the layers structure of the OSI model. In fact, in each of said protocols, a certain source layer will divide the data it receives from an upper layer adding to said data a header e/o a tail and will forward all this to a lower layer. On the destination side the opposite operations will occur.

Therefore, herebelow reference will be made to the conceptual OSI model for ease of reference; it is to be understood that what it will be described will be easily suitable for every application protocol with obvious modifications, typical of the relation existing between each application protocol and the OSI standard.

Monitoring systems for data transmitted between a sender node and a destination node are already known. However, said systems can only analyze the OSI layers 2 (data link) and 3 (network). The monitoring and the successive interpretation

of the data at said layers allow only the monitoring of anomalies in the exchange protocol among the various components of a network data transmission system.

Therefore, a typical disadvantage of said prior art systems is their incapability of decoding the application piece of information transported on the network, i.e., the piece of information related to the layers 4 to 7 of the OSI standard.

With reference to the OSI standard, the communication unit in a network is the packet. Packets are in turn divided into frames. The beginning and the end of each frame are usually determined by delimitation characters. The frames are in turn divided into information frames and control frames. The information frames transport the data related to the message that is to be transmitted throughout the network, while the control frames deal with the regulating modes of said transport, i.e., the flow control and the starting of the error recovery actions. Both the information frames and the control frames contain a header portion identifying the frame type and a body portion which is typical of the frame itself.

The information frame structure will be described with reference to figure 3. In the upper portion of said figure the generic structure of an OSI layer packet 2 is schematically described, thus comprising both information frames 1 and control frames 2. A single information frame (OSI layer 3) is constituted by a header portion 3, containing the identification that the frame is an information frame, and by a body portion 4. The body portion (OSI layers 4 to 7) contains the real message 5, together with a plurality of fields 6, typical of the particular application syntax used, illustrated by way of example in the figure with the characters C1, C2 and C3. The application syntax is the information relative to the number of fields contained within the plurality 6, to the meaning of each of said fields and to the data contained therein.

Reference will be now made to figure 4, showing a block diagram of the component for monitoring and interpretation of application protocols belonging to the apparatus according to the present invention. In said figure first of all a source node 7 and a destination node 8, terminals of the network portion in which the data are monitored and interpreted, are shown. Throughout the connection between said two nodes, schematically illustrated by arrows F3, F4, F5, F6 and by the transmission medium 23, data relative to plural communications between a first set of source processors (not shown in figure) upstream of the source node 7 and a second set of destination processors (not shown in the figure) downstream of the destination node 8 travel bidirectionally.

Said data are monitored by means of a data monitoring device 9. Several are the monitoring devices known on the market; for instance, as for the

networks based on Ethernet technology, the Fast Etherlink XL™ card produced by the company 3Com can be mentioned. As for the networks based on X.25 technology, for example the S508 card produced by the Canadian company Sangoma™. Said card can operate with different OSI layer 1 (physical layer) standards such as, for example, the RS232 (or V.24) standard and the RS422 (or V.35) standard. The OSI layer 2 (data link) standards together with which said card can operate are, for example, the HDLC standard and the X.25 standard. Anyway, the kinds of data monitoring device 9 to be chosen for the purposes of the present invention can vary depending on which OSI layers 1 or 2 standards one needs to operate. In fact, it will be possible to use monitoring devices working with implementation standards different from the OSI layer 2, such as for example "Frame Relay" or SDLC or also BSC and the like. Said devices are well known to the person skilled in the art and they will not be here described in detail.

The monitoring occurs "transparently" by means of two parallel connectors 10 and 11, schematically illustrated in the figure, for monitoring of the data coming respectively from the source node 7 and from the destination node 8. The monitoring device 9, shown by the dashed block in the figure, includes a source data receiver 12, a destination data receiver 13 and a connection interface 14. The source data receiver 12 allows the reception of the data coming from the source node 7 only, as it is schematically indicated with the arrow F7; on the other hand, the destination data receiver 13 allows the reception of the data coming from the destination node 8 only, as schematically indicated with the arrow F8. The data received in this manner are transmitted to the connection interface 14, as it is indicated by arrows F9 and F10.

Each data packet situated at a layer corresponding to the OSI layer 2 read by the monitoring unit 9 is forwarded to a control unit 15, as indicated by arrow F11. The operation of the control unit 15 will be described in detail later. To each of said packets a reading time is associated by means of a dating unit 16, represented outside the control unit 15 for ease of description and therewith connected as indicated by arrow F12. Such dating unit 16 can be any absolute timing device available on the market, in particular a radio or satellite one. In a preferred embodiment of the present invention a radio controlled digital clock adjusted on the CET (Central European Time) broadcast by a geostationary satellite was used.

Further to the association of the reading time by means of the dating unit 16, the control unit 15 orders in a logical way the single frames so as to reconstruct the right logical and time sequence of the sending of the frames that, as it is known, does not always coincide with the reception sequence: in fact, due to the forwarding

techniques along telecommunication networks, it is possible for a forwarded sequence of the "ABC" kind to be received in all of its possible permutations, i.e., "ABC", "ACB", "BAC", "BCA", "CAB", "CBA". Then the control unit 15 discriminates the information frames from the control frames. For example, if transmission of the information occurs in the HDLC language, the last bit of the header portion of an information frame is 0 whereas the last bit of the header portion of a control frame is 1. Therefore, inside the control unit 15 there are means, not described in the figure, discriminating said last bit, e.g. a firmware contained in a ROM. In any case, no matter which data transmission code is used, it will always be possible to provide means for said discrimination discriminating a control frame from an information frame. Therefore, said discrimination allows to store the single information frames deprived of the header portion and comprising the body portion only, thus containing the information which is typical of the particular application syntax used, together with the message to be transmitted.

The data incorporating the monitoring time and divided into information frames and control frames are stored inside a discriminated data storing unit 17, bidirectionally connected to the control unit 15 as indicated by arrow F13. There is also a predetermined data storing unit 18, bidirectionally connected to the control unit 15. Said predetermined data represent possible interpretations of the information or control frames contained in the discriminated data storing unit 17. Their use will be explained herebelow with reference to the following figures. The connection between the predetermined data storing unit 18 and the control unit 15 is indicated by arrow F14.

Reference will be now made to figure 5, showing a flow chart indicating the operations executed by the control unit 15 on the information frames stored in the data storing unit 17. It is to be understood that the access to such information frame can be selectively regulated by means of authorizations and privileges management systems such as passwords, encryption and decryption codes, badge readers and the like given to qualified users.

A first step S1 indicates the reading of the various packets by the monitoring unit 3. A second step S2 indicates the previously described discrimination, operated by the control unit 15 between the information frames and the control frames, together with the association of the monitoring time.

On the non-application low layer control frames, whose use is unimportant for the purposes of the present invention, a statistic processing might also be provided, operated in the step S3. Said processing is not described in detail at

the moment; the modes by which it occurs will turn out to be clear at the end of the present description. The final result of such processing will provide a list of the various control frames, reporting also the number of occurrences for each of said frames.

As for the information frames, the flow proceeds to a step S4 wherein the single information frames are reconstructed according to their specific application syntax. To the purposes of said reconstruction, the application syntax structures of the single information frames must be known. In fact, they are contained inside the predetermined data storing unit 18 described with reference to the previous figure 3. Said unit 18 contains, for example in a text file, a formal abstract description for possible interpretations of the information or control frames. Said data represent the modes according to which the body portion of a single information frame can be structured, for instance the machine transmission code (i.e., related to an information frame forwarded by the source or the destination), the number of the channel (i.e., related to a specific processor upstream of the source node or to a specific processor downstream of the destination node), protocol numbers, data processing numbers etc. said unit 18 can of course contain the syntax of several application protocols, of the information frames that are to be reconstructed in that moment.

A reconstruction of the information frames one by one is obtained by a sequential comparison of the body portion of each information frame with each one of the abstract models in the unit 18.

Further to this, the different application sequences occurred between a determined source processor and a determined destination processor can be reconstructed, i.e., ordered according to time and kind of communication. Throughout the present description, for application sequence will be intended the whole of the information frames exchanged between a determined source processor and a determined destination processor during a single communication. The application sequence ordered in step S5 will contain the single information frames ordered according to a time criterion only and not also to a logical one. Ordering by time will be possible through the time association occurred in the previous step S2.

To give also a logical ordering of the data inside a specific application sequence, the presence of a group of application rules directing the data exchange between source and destination can be useful, although not necessary. Said application rules, typical of the particular kind of conversation between a determined source processor and a certain destination processor, must be predetermined and as such they as well are collected in the predetermined data storing unit 18. Said

application rules are a series of possible interpretations of the information frames sequences contained in the discriminated data storing unit 17.

Reference will be now made to an electronic purchase of a certificate (personal data, cadastral ...) the cost of which is regulated by means of a POS payment. In this case it will be necessary to:

1) Apply for the certificate to the service provider (FDS), i.e., to the body issuing the certificate;

2) Acquire from FDS the cost of the certificate;

3) Operate the payment of said cost by means of the POS component;

4) Communicate to FDS the executed payment;

5) Verify the actual transmission of the certificate from FDS to the applicant (as for the certificate validity and authenticity techniques such as the "digital signature" might be used);

6) Credit the cost, by means of the POS component, to the bank account of FDS.

If the apparatus object of the present invention serves several service providers, the POS component could not communicate directly with the bank of the service provider (FDS), but instead with a "service center" to which, with simple modifications of the POS management software, it shall forward all the amounts and the codes of the FDS.

The same "service center" will be in charge of the crediting to the single bank accounts of the various service providers. Thus, all the communications of the apparatuses which are on the territory will be addressable to the same service center. The service center will sum up all the amounts relative to the single providers and credit their bank accounts.

In the present example FDS is assumed to be the only one (e.g., operating by an Intranet). In particular, FDS is assumed to be offering a certificate distribution service by means of a countrywide network of "unattended counters". It will be possible to apply for a certificate at any time, from every counter, even a certificate referring to a territorial zone different from the one where the counter is located, operate the related payment and obtain what was applied for. A counter is represented by any location, located in any one site (public or private) provided with the apparatus object of the present invention.

Each one of the above described steps (certificate application, cost acquisition, payment operation...) is realized by means of the exchange between applicant and provider of application flows that are codified in frames. As previously

described, the apparatus object of the present invention can reconstruct said application sequences.

Herebelow the single steps and roles undertaken by the various components are reported.

1) Certificate request

- Applicant: unattended counter
- Provider: body issuing the certificate

The reconstruction of the application flows (sequences) refers to data exchanged between the "applicant" counter from which the certificate application is operated and the "provider" managing the dialogue needed to acquire the information to monitor and issue the certificate.

Furthermore, the apparatus object of the present invention stores the reconstructed data. Data for the applicant identification are particularly important.

2) Acquisition of the certificate cost:

- Applicant: unattended counter
- Provider: body issuing the certificate

The reconstruction of the application flows (sequences) refers to data exchanged between the "applicant" counter from which the certificate application is operated and the "provider" that, once the certificate is individuated, requests the payment thereof.

The apparatus object of the present invention further stores all the reconstructed data. Data referring to the requested amount are particularly important.

3) Payment operation

- Applicant: unattended counter
- Provider: center of the card issuing company

The reconstruction of the application flows (sequences) refers to data exchanged between the "applicant", counter from which the application for the certificate to be paid was operated, and the "provider" which has to authorize the payment. It is worth to point out that this time the provider is different from the previous cases and that the apparatus constitutes the interface for the coupling between the authority issuing the certificate and the one authorizing the payment.

The apparatus object of the present invention further stores all the reconstructed data. Data referring to the amount authorized by the issuer are particularly important.

4) Communication to the service provider of the executed payment

- Applicant: unattended counter

- Provider: body issuing the certificate

The reconstruction of the application flows (sequences) refers to data exchanged between the "applicant", communicating data of the executed payment to the "provider" that, on these bases, is authorized to send the certificate.

The apparatus object of the present invention further stores all the reconstructed data.

5) Verification of the actual transmission of the certificate

- Applicant: unattended counter

- Provider: body issuing the certificate

The reconstruction of the application flows (sequences) refers to data exchanged between the "provider", sending data related to the certificate and the "applicant" verifying the actual reception.

The apparatus object of the present invention further stores all the reconstructed data. Data related to the certificate reception and content are particularly important.

6) Crediting, by means of the POS component, to the bank account of FDS

- Applicant: unattended counter

- Provider: bank (or service center) of FDS

The reconstruction of the application flows (sequences) refers to data exchanged between the "applicant", sending data related to the payments related to a determined time interval and the "provider" acquiring the data and acknowledging the reception thereof.

The apparatus object of the present invention further stores all the reconstructed data. Data related to the transmitted amount are particularly important.

Obviously, every step consists of the exchange of different application sequences, each one reconstructed on the basis of suitable rules. In fact, the step of application for a certificate will be divided into entering the certificate type, the holder's data, residence etc. Likewise, the other steps as well shall be divided into various substeps.

An example of the application rules is reported in the following table 1, wherein reference is made to the step of applying for a certificate, substep holder's data entering. The source represents a user (client) applying for a certificate, the receiver (provider) represents the service provider (body qualified to issue the certificate). It is supposed that the conversation is codified by means of the application rules stored inside the predetermined data storing unit 18.

TABLE 1

1: AS ? FDS 15 AS ? FDS 5 AS ? FDS 0 Data of the certificate holder were regularly entered
.....
.....
4: AS ? FDS 13 AS ? FDS 0 Domicile entered by the applicant does not correspond
.....
.....
.....

Every line of said table is an application rule, indicating i.e. a possible data exchange application sequence between source and destination. The meaning of each application sequence is illustrated herebelow. For example, the first line indicates the following sequence of information frames:

- the source (AS) interrogates (?) the destination;
- the destination (FDS) answers with the activity number 15 codifying, e.g., the request of entering the forename of the certificate holder;
- the source (AS) interrogates again (?) the destination;
- the destination (FDS) answers with the activity number 5 codifying, e.g., the request of entering the surname of the certificate holder;
- the source (AS) interrogates (?) the destination; and
- the destination (FDS) answers with the activity number 0 codifying the sequence completion.

The result obtained at the end of this conversation is that data of the certificate holder have been entered correctly.

The merely exemplifying table 1 could be represented also with a tree structure with more or less branches, according to the number of application sequences provided. Every path up to the leaves of the tree would then represent a particular application sequence, i.e., a particular conversation between source and receiver, i.e., again a particular sequence of information frames between source and receiver.

The number of application rules can be anyone. The larger the number of application rules provided, the bigger the chance to associate each of the application sequences temporally reconstructed in the step S5 with a well defined logical meaning, found by comparison with a particular application rule contained in

the predetermined data storing unit 18 in figure 3. Therefore, in this manner it will be possible to verify the correctness or the anomaly of the particular application sequence that is being compared in that moment.

In the step S6 in figure 5 first of all the control unit 15 verifies whether such application rules are available or not. Supposing that said application rules are known, the flow can proceed either toward a step S8 or toward a step S9, depending on what was chosen in the step S7. The step S8 allows a simple classification of the application sequences. In fact, each application sequence is classified as belonging to a particular path among the various possible paths inside the application rules tree. The step S8 will be explained in greater detail with reference to the following figure 6.

On the other hand, in the step S9 the logical path of all the application sequences monitored by the apparatus in a predetermined time interval is reconstructed. Said step S9 will be described in greater detail with reference to the following figure 7.

The apparatus according to the present invention allows a reconstruction of the logical path of the application sequences also if a series of application rules is not provided. In this event, the flow proceeds toward a step S10, that will also be described later.

Reference will be now made to figure 6, which provides a more detailed explanation of what was previously described with reference to the step S8 in figure 5. In a first step S11 the single application sequence, object of the comparison, is selected. In a successive step S12 the elements which are characterizing for comparison purposes are selected inside the selected application sequence.

In the previously described example of purchase with reference to table 1 said characterizing elements might be: the identification number of the source processor, the identification number of the user who required the operation of purchase, the data provided by the source and the data provided by the destination.

In the step S13 the characterizing elements of the application sequence at issue are compared with one of the application rules of the above described table 1, searching for a possible correspondence. If such a correspondence is found, the flow proceeds toward a step S14 in which said correspondence is reported and will have to be taken into consideration in the results of the interpretation. Then the flow selects another sequence and executes again the step S11. If the correspondence at the step S13 is not found the control unit 15 goes in step S15 to a subsequent rule,

and if (step S16) there are still rules allowing a comparison, the control unit executes once again the comparison of step S13. If no further rules are found, the control unit reports an anomaly in the step S17. Such an anomaly might alternatively mean:

- either a kind of sequence which should have not been occurred (a real anomaly); or

- a kind of sequence not inserted by mistake inside the application rules tree.

In each of said events finding such an anomaly is certainly useful for the certification of the kinds of application sequences occurred in the network portion under examination.

Reference will be now made to the following figure 6 which gives a more detailed explanation of what described in the step S9 in figure 5.

The steps S18 and S19 select respectively the single application sequence and the characterizing elements of the same, similarly to what described with reference to the previous figure 5. The step S20 is to indicate the comparison between the application sequence and the preset application rules contained inside the predetermined data storing unit 18. If a correspondence is found, the flow proceeds toward a step S21 wherein the correspondence found is taken into consideration through the update of the related statistic fields. Steps S18-S20 will be subsequently repeated, until the end of the sequences to be classified. If no correspondence is found, the application sequence to be classified is new; it can be an anomaly or simply an unexpected sequence. In this event the flow proceeds toward a step S22 wherein the statistic fields related to that specific sequence are initialized. Furthermore, the new sequence will be inserted in the list of the preset sequences to be used for the comparison in the step S20. This is also indicated by the double pointing of the arrow F14 in the previous figure 4. Said particular sequences, i.e. the possible anomalies, can be evidenced in a particular manner to be recognized as such. Further to this, also in this case the steps S18-S20 are repeated until the end of the sequences to be classified. In particular, besides the number of crossings for each tree branch, it is also possible to monitor uncrossed branches.

In case there is no preset sequence of application rules, it will always be possible for the control unit to reconstruct the communication applications occurred in the network portion under control (step S9 in figure 5). In this event, each analyzed application sequence will not be compared with the preset sequences, but with the previously analyzed sequences. Therefore, the tree structure containing statistical information will be reconstructed by means of reciprocal comparison of each body portion of the information frames with the others. Also in this case, a tree

will be constructed and it will be possible to know the number of crossings for each branch. Obviously, in this case it will not be possible to monitor the uncrossed branches as there will not be a prior knowledge of the existence of said branches.

Reference will be now made to figures 8A and 8B showing respectively an example of an information frame structure and an example of a tree structure containing statistic information obtained by means of the apparatus according to the present invention.

In figure 8A it is possible to notice four different fields: a first field 19 indicating the name of the source or destination processor; a second field 20 indicating the number of connections in the monitored time interval, a third field 21 indicating the average time length of each connection, counted for example in milliseconds, and a fourth field 22 indicating the code of the activity executed.

Figure 8B indicates the reconstructed tree. A first element E1 in the tree indicates that AS (source) connected 20 times, with an average connection time of 0 milliseconds (simple opening of the connection with the destination) and executed the activity with the code 0. A second element E2, E1's only "son", indicates that in all those 20 connections FDS (destination) answered with the activity having the code 20, with an average connection time of 20 milliseconds. There were two manners of proceeding. AS answered 18 times (element E3) with the activity 0 and twice (element E4) with the activity 1. The tree proceeds with other elements, whose meaning is now clarified by the context. The tree herewith disclosed is the result of the logical ordering operated in the step S9 or S10 in figure 5.

It is to be noted that the monitoring of the contents in the fields 19 and 22 of each element was operated in the step S4 in figure 5. The monitoring of the connections among the various elements, i.e., the fact that the element E2 is E1's "son" and that the elements E3 and E4 are E2's "sons", was operated either in the step S9 or in the step S10 in figure 5.

The data flow relating to a particular application intercurred between one or more determined processors upstream of a source node and one or more determined processors downstream of a destination node can be therefore reconstructed, in the sense of univocally determined in all its component parts. Therefore, what is reconstructed is the conversation relating to one or more client/provider applications. The logical reconstruction can take the form of the tree structure of figure 8B. Thus, communications relating to different applications (which therefore originate different application trees) can be reconstructed, and on the same source processor also more client-applications (relating to different

provider-applications) can be present. In the same way, on a destination processor more provider applications can be present.

Figure 9 shows a schematic view of the apparatus according to the present invention. One or more processors 24 are connected in local network to the apparatus 25 according to the present invention, including a POS 26 and an apparatus 27 for monitoring and interpretation of application protocols according to what described with reference to the previous figures from 2 to 8B. In particular, the schematic representation of the apparatus 27 corresponds to the representation thereof shown in figure 4. The POS 26 includes a modem 28 and it is connected to the apparatus 27 by means of a local connection 29. In particular it is to be provided that both the POS 26 and the apparatus for monitoring and interpretation 27 comprise respective local network interfaces 37, 38 (as e.g. the Fast Etherlink XL™ card produced by the company 3Com™) coupled therebetween by means of a hub 39. The local network interface 38 of the apparatus 27 is to be understood as connected to the control unit 15 of the apparatus itself. The POS 26 further includes an electronic card reading device, not shown in figure. The modem 28 is in turn connected to the center 30 of the card issuing company by means of a telephone connection 31. The apparatus 27 is connected to the local network, of which the processors 24 take part, by means of parallel connectors 10, 11 identical to those already described with reference to the previous figure 4. The local network of processors 24 is then connected to a router 32 by a connection 33. The task of the router 32 is that of routing the various local networks toward the Internet/Intranet/Extranet network, or anyhow toward any remote access to a service provider, schematically represented with 34, and from it to the trader 35. The router 32 will be connected on the one hand to the local network 24 and on the other hand to the geographical network by means of a dedicated interface (telephone, ISDN, CDN dedicated line, optical fibers dedicated line or the like). If the processor 24 is alone (not connected to a local network) then the router can be made superfluous by providing the user system with an internal modem of its own for connection to the geographical network.

The operation of the system in figure 9 will be better explained with reference to the flow charts in figures 10A and 10B.

In a step D14 the user selects the product/ service of interest from an interface of the WEB or other kind, through the processor 24 connected to the Internet, Intranet, Extranet network or the like.

The processor 24, through which the client makes his choice, can in turn be connected or not to a local network with other processors/devices, as previously represented with reference to figure 9.

In a successive step D15 the apparatus 25 in figure 9 automatically acquires and stores all information related to the requested transaction by means of the component for monitoring and interpretation of the application protocols 27, among which the features of the item to be purchased, the trader, the amount of the requested payment etc. The manner according to which such an automatic acquisition occurs have already been described with reference to the previous figures from 2 to 8B, concerning in particular the temporal and logical ordering of the monitored data, as well as the association of a logical meaning to said data using the application rules. Therefore, the answer of the trader to the request of the product/service operated by the client will be reconstructed and data of interest will be individuated among the reconstructed and stored application sequences.

In a subsequent step D16 the user/client inserts his payment card in the reading device in POS 26.

In a subsequent decision step D17 the card is recognized or not.

If the card is recognized the flow proceeds to the steps D18 and D19 wherein respectively the entering (manual or automatic through communication by apparatus 25) of the amount to be paid and of the secret code are requested. The entering of the amount to be paid (step D18) is also acquired and stored by the component 27 for monitoring and interpretation of the application protocols.

In a successive decision step D20 the secret code is recognized or not.

In a successive step D21 the acquired information are forwarded to the center of the card issuing company 30 in figure 9. Said information include the client code, the amount to be paid, the identification number of the caller and any other data that needs to be processed by the side of the center 30.

It is important to note that the path of the information related to the step D21 occurs by use of a communication channel (indicated with 31 in figure 9) that can differ from the one (indicated with 36 in figure 9) used for the connection to Internet, Intranet, Extranet or the like. For instance, such a path can occur through the ISDN channel "D", as it is a safe and advantageous solution, as a matter of fact already used in the POS systems of the known art. Other manners can for example provide a connection of the mobile phone, satellite, on RTG, on a dedicated channel type, or any other technique available now or in the future.

In the successive steps the center 30 acquires the request, processes it and sends an answer to the caller.

In particular, in step D22 it is verified whether the data available by the center 30 authorize the transaction or not. If the transaction is authorized, in a step D23 the debiting of the cost on the center side occurs. Making reference herebelow to figure 10B, in a successive step D24 the acquisition by the user of the affirmative answer occurs.

In a subsequent step D25 the comparison between the requested amount (stored in step D15) and the paid amount occurs. Said comparison occurs by means of the component 27 for monitoring and interpretation of the application protocols (figure 9) and can concern the comparison between the requested data and those of the product that is about to be received. Thus, an automatic congruency control of the paid amount and the purchased item is ensured.

In the event of a positive comparison, in a successive step D26 the communication to the trader 35 (figure 9) of the executed payment and therefore the authorization to the trader to consign the goods occurs.

In a subsequent step D27 the storing of the transaction data in the component 27 occurs. Said storing, like the acquisitions and storages hereto described with reference to the component 27, occurs in a sealed local memory on the user side, to be opened for possible controls or disputes. Said memory, not shown in figure 9, is not described in detail here, as the implementation thereof is obvious for the person skilled in the field.

In a subsequent step D28 the forwarding of the purchased product is provided. If said product is an electronic document or anyhow an information obtainable via network, said product is forwarded directly to the processor 24 of the user.

If instead the product is to be delivered later on (through the usual distribution channels), anyhow the provider will have the advantage of having already acquired the certain payment, and the purchaser the advantage of having a system capable of documenting the operated transaction, therefore being in all respects a proof of the order, to be used in case of failed delivery.

The subsequent steps D29, D30 and D31 can provide the printing of the payment receipt, the printing of the description of the purchased item and the printing of the possibly requested electronic document, respectively.

From time to time the apparatus object of the present invention will forward the credit resulting from the sum of the various purchases operated at the bank of the provider of products/services.

The crediting can occur either to a single trader (e.g. a Ministry, a bank or a local authority) or to more traders, the latter being usual in the electronic trade on Internet. In case of crediting to various traders, two modes can be provided:

1) A "service center" for all the operated transactions, where the crediting due to each trader are divided (according to what hereto described)

2) Communicate the transaction data directly to the traders or to the banks thereof, once the OK to the payment and to the sending of the goods is obtained.

The present invention has been up to now described with reference to one of its embodiments, given as a non-limiting example.

Furthermore, it is to be understood that there are other possible embodiments falling within the protective scope of the present industrial property right.